EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Beatrice L. Koempel-Thomas on 7/27/09.

The application has been amended as follows:

Claims 1, 13-16, 18, 19, 22, 24-29, 31, 32, 34, 36-39, 42, and 43 have been amended by this Examiner's Amendment.

Claims:

1. **(Currently Amended)** A computer implemented method comprising:

establishing, via the computer, at least one cryptography service parameter threshold comprising a minimum level of security;

establishing, via the computer, at least one maximum cryptography service parameter threshold;

wherein establishing said at least one of either said minimum or maximum cryptography service parameter threshold includes establishing a plurality of correctness categories, wherein each at least one of said plurality of correctness

categories includes at least one cryptography algorithm identifier and said plurality of correctness categories includes at least one correctness category selected from a group of correctness categories consisting of authorized algorithms, unauthorized algorithms, weak algorithms, and strong algorithms;

maintaining said at least one of said minimum and maximum cryptography service parameter thresholds in memory;

selectively detecting, via the computer, a request from an application submitted via an application programming interface to an operating system of the computer, the request comprising a request for at least one cryptography service at the computer; and

selectively performing, via the computer, at least one correctness detection action responsive to detecting the request based on the requested cryptography service and the at least one cryptography service parameter threshold in the memory, wherein:

the at least one correctness detection action selectively performed includes suggesting at least one alternative cryptography service;

the at least one alternative cryptography service comprises a cryptography service which meets the minimum level of security; and

the selectively performing at least one correctness detection action based on the requested cryptography service and the at least one cryptography service parameter threshold in the memory includes determining if a cryptographic key associated with the requested cryptography service is suitable for use based on the at least one cryptography service parameter threshold in the memory, wherein determining if the cryptographic key associated with the requested

cryptography service is suitable for use based on the at least one cryptography service parameter threshold in the memory includes comparing a size of the cryptographic key with the at least one cryptography service parameter threshold in the memory, wherein the size of the cryptographic key is identified by bit length.

2. (Previously Presented) The computer implemented method as recited in Claim 1, wherein establishing, via the computer, said at least one cryptography service parameter threshold includes at least identifying unacceptable cryptography algorithms.

3. (Previously Presented) The computer implemented method as recited in Claim 1, wherein establishing, via the computer, said at least one cryptography service parameter threshold includes at least identifying acceptable cryptography algorithms.

4 - 7. (Canceled)

8. (Previously Presented) The computer implemented method as recited in Claim 1, wherein establishing, via the computer, said at least one cryptography service parameter threshold includes at least identifying at least one acceptable seed size parameter.

9. (Previously Presented) The computer implemented method as recited in Claim 1, wherein establishing, via the computer, said at least one cryptography service parameter threshold includes at least identifying at least one unacceptable seed size parameter.

10. (Previously Presented) The computer implemented method as recited in Claim 1, wherein selectively detecting, via the computer, said request for at least one cryptography service includes monitoring at least one process selected from a group of processes comprising an application, an operating system, a cryptography system service, and another process calling into the cryptography application programming interfaces.

11 - 12. (Canceled)

13. (Currently Amended) The computer implemented method as recited in Claim 1, wherein selectively performing, via the computer, said at least one correctness detection action based on said requested cryptography service and said at least one cryptography service parameter threshold in the memory includes determining if a cryptographic algorithm associated with said requested cryptography service is suitable for use based on said at least one cryptography service parameter threshold in the memory.

14. (Currently Amended) The computer implemented method as recited in Claim 13, wherein determining if said cryptographic algorithm associated with said requested cryptography service is suitable for use based on said at least one cryptography service parameter threshold in the memory further includes comparing a cryptography algorithm identifier with said at least one cryptography service parameter threshold in the memory.

15. (Currently Amended) The computer implemented method as recited in Claim 1, wherein selectively performing, via the computer, said at least one correctness detection action based on said requested cryptography service and said at least one cryptography service parameter threshold in the memory includes performing at least one action selected from a group of actions consisting of:

interrupting at least one process;

stopping at least one process;

starting at least one process;

displaying alert information;

logging alert information;

suggesting at least one alternative cryptography service;

outputting alert messages;

causing alteration of a graphical user interface; and

forcing use of at least one other cryptography service.

16. (Currently Amended) A computer readable medium having computer-implementable instructions embodied thereon, which when executed cause one or more processing units to perform acts comprising:

establishing at least one cryptography service parameter threshold comprising a minimum cryptography service parameter threshold;

establishing at least one maximum cryptography service parameter threshold;

wherein establishing said at least one of either said minimum or maximum cryptography service parameter threshold includes establishing a plurality of correctness categories, wherein each at least one of said plurality of correctness categories includes at least one cryptography algorithm identifier and said plurality of correctness categories includes at least one correctness category selected from a group of correctness categories consisting of authorized algorithms, unauthorized algorithms, weak algorithms, and strong algorithms;

maintaining said at least one of said minimum and maximum cryptography service parameter thresholds in memory;

selectively detecting a request from an application submitted via an application programming interface to an operating system, the request comprising a request for at least one cryptography service; and

selectively performing at least one correctness detection action responsive to detecting the request based on said requested cryptography service and said at least one ~~minimum cryptography service parameter threshold and said at least one maximum~~ cryptography service parameter threshold in the memory, wherein:

the at least one correctness detection action selectively performed includes forcing use of at least one alternative cryptography service;

the at least one alternative cryptography service comprises a cryptography service which meets the minimum level of security; and

the selectively performing at least one correctness detection action based on the requested cryptography service and the at least one cryptography service parameter threshold in the memory includes determining if a cryptographic key associated with the requested cryptography service is suitable for use based on the at least one cryptography service parameter threshold in the memory, wherein determining if the cryptographic key associated with the requested cryptography service is suitable for use based on the at least one cryptography service parameter threshold in the memory includes comparing a size of the cryptographic key with the at least one cryptography service parameter threshold in the memory, wherein the size of the cryptographic key is identified by bit length.

17. (Canceled)

18. (Currently Amended) The computer readable medium as recited in Claim [[17]] 16, wherein establishing said at least one of either said minimum or maximum cryptography service parameter threshold includes at least one of the following acts:

identifying unacceptable cryptography algorithms; and

identifying acceptable cryptography algorithms.

19. (Currently Amended) The computer readable medium as recited in Claim [[17]] 16, wherein establishing said at least one of either said minimum or maximum cryptography service parameter threshold includes at least one of the following acts:

identifying at least one unacceptable cryptography key size parameter; and

identifying at least one acceptable cryptography key size parameter.

20 - 21. (Canceled)

22. (Currently Amended) The computer readable medium as recited in Claim [[17]] 16, wherein establishing said at least one of either said minimum or maximum cryptography service parameter threshold includes at least one of the following acts:

identifying at least one acceptable seed size parameter; and

identifying at least one unacceptable seed size parameter.

23. (Original) The computer readable medium as recited in Claim 16, wherein selectively detecting said request for at least one cryptography service includes monitoring at least one process selected from a group of processes comprising an application, an operating system, a cryptography algorithm, and a cryptography application programming interface.

24. (Currently Amended) The computer readable medium as recited in Claim 16, wherein selectively performing said at least one correctness detection action based on said requested cryptography service if said requested cryptography service does not satisfy said at least one cryptography service parameter threshold in the memory includes determining if a cryptographic key associated with said requested cryptography service is suitable for use based on said at least one cryptography service parameter threshold in the memory.

25. (Currently Amended) The computer readable medium as recited in Claim 24, wherein determining if said cryptographic key associated with said requested cryptography service is suitable for use based on said at least one cryptography service parameter threshold in the memory includes comparing a size of said cryptographic key with said at least one cryptography service parameter threshold in the memory.

26. (Currently Amended) The computer readable medium as recited in Claim 16, wherein selectively performing said at least one correctness detection action based on said requested cryptography service if said requested cryptography service does not satisfy said at least one cryptography service parameter threshold in the memory includes determining if a cryptographic algorithm associated with said requested cryptography service is suitable for use based on said at least one cryptography service parameter threshold in the memory.

27. (Currently Amended) The computer readable medium as recited in Claim 26, wherein determining if said cryptographic algorithm associated with said requested cryptography service is suitable for use based on said at least one cryptography service parameter threshold in the memory further includes comparing a cryptography algorithm identifier with said at least one cryptography service parameter threshold in the memory.

28. (Currently Amended) The computer readable medium as recited in Claim 16, wherein selectively performing said at least one correctness detection action based on said requested cryptography service if said requested cryptography service does not satisfy said at least one cryptography service parameter threshold in the memory includes performing at least one action selected from a group of actions consisting of: interrupting at least one process, stopping at least one process, starting at least one process, displaying alert information, logging alert information, suggesting at least one alternative cryptography service, outputting alert messages, and causing alteration of a graphical user interface.

29. (Currently Amended) An apparatus comprising:

a system memory;

a processing unit; and

~~cryptography correctness detection logic~~ programmable instructions stored on the system memory and executable by the processing unit to ~~configured~~ configure the apparatus to:

establish at least one cryptography service parameter threshold, wherein the at least one cryptography service parameter threshold comprises a threshold setting a minimum level of security;

establish at least one maximum cryptography service parameter threshold;

maintain said at least one of said minimum and maximum [[one]] cryptography service parameter thresholds in said memory; and

establish a plurality of correctness categories in said memory, wherein each at least one of said plurality of correctness categories includes at least one cryptography algorithm identifier wherein said plurality of correctness categories includes at least one correctness category selected from a group of correctness categories consisting of authorized algorithms, unauthorized algorithms, weak algorithms, and strong algorithms;

selectively detect a request for at least one cryptography service; and

selectively perform at least one correctness detection action based on said requested cryptography service if said requested cryptography service does not satisfy [[the]] at least one cryptography service parameter threshold in said memory, wherein the at least one correctness detection action selectively performed includes forcing use of at least one other cryptography service, wherein the at least one other cryptography

service comprises a cryptography service having a higher level of security than represented by the cryptography service parameter threshold.

30. (Canceled)

31. (Currently Amended) The apparatus as recited in Claim [[30]] 29, wherein said cryptography correctness detection logic is further configured to identify at least one of the following: at least one unacceptable cryptography algorithm, and at least one acceptable cryptography algorithm.

32. (Currently Amended) The apparatus as recited in Claim [[30]] 29, wherein said cryptography correctness detection logic is further configured to identify at least one of the following: at least one unacceptable cryptography key size parameter; and at least one acceptable cryptography key size parameter.

33. (Canceled)

34. (Currently Amended) The apparatus as recited in Claim [[30]] 29, wherein said cryptography correctness detection logic is further configured to identify at least one of the following: at least one acceptable seed size parameter; and at least one unacceptable seed size parameter.

35. (Original) The apparatus as recited in Claim 29, wherein said cryptography correctness detection logic is further configured to monitor at least one process selected from a group of processes comprising an application, an operating system, a cryptography algorithm, and a cryptography application programming interface.

36. (Currently Amended) The apparatus as recited in Claim 29, wherein said cryptography correctness detection logic is further configured to determine if a cryptographic key associated with said requested cryptography service is suitable for use based on said at least one cryptography service parameter threshold in said memory.

37. (Currently Amended) The apparatus as recited in Claim 36, wherein said cryptography correctness detection logic is further configured to compare a size of said cryptographic key with said at least one cryptography service parameter threshold in said memory.

38. (Currently Amended) The apparatus as recited in Claim 29, wherein said cryptography correctness detection logic is further configured to determine if a cryptographic algorithm associated with said requested cryptography service is suitable for use based on said at least one cryptography service parameter threshold in said memory.

39. (Currently Amended) The apparatus as recited in Claim 38, wherein said cryptography correctness detection logic is further configured to compare a cryptography algorithm identifier with said at least one cryptography service parameter threshold in said memory.

40. (Previously Presented) The apparatus as recited in Claim 29, wherein said cryptography correctness detection logic is further configured to use at least one action selected from a group of actions consisting of:

interrupting at least one process,

stopping at least one process,

starting at least one process,

displaying alert information,

logging alert information,

suggesting at least one alternative cryptography service,

outputting alert messages, and

causing alteration of a graphical user interface, to be performed.

41. (Previously Presented) The method as recited in Claim 1, wherein:
in an event that the cryptography service is an asymmetric cryptography service, the minimum level of security comprises a minimum acceptable public key size of at least 1024 bits; and in an event that the cryptography service is a symmetric cryptography

service, the minimum level of security comprises a minimum acceptable symmetric key size of at least 128 bits.

42. (Currently Amended) The computer readable medium as recited in Claim 16, wherein: the at least one alternative cryptography service comprises a cryptography service which meets the minimum level of security; and the selectively performing at least one correctness detection action based on the requested cryptography service and the at least one cryptography service parameter threshold in the memory includes determining if a cryptographic key associated with the requested cryptography service is suitable for use based on the at least one cryptography service parameter threshold in the memory, wherein determining if the cryptographic key associated with the requested cryptography service is suitable for use based on the at least one cryptography service parameter threshold in the memory includes comparing a size of the cryptographic key with the at least one cryptography service parameter threshold in the memory, wherein the size of the cryptographic key is identified by bit length.

43. (Currently Amended) The apparatus of claim 29 wherein the selectively performing at least one correctness detection action based on the requested cryptography service and the at least one cryptography service parameter threshold in said memory includes determining if a cryptographic key associated with the requested cryptography service is suitable for use based on the at least one cryptography service parameter threshold in said memory, wherein determining if the cryptographic key

associated with the requested cryptography service is suitable for use based on the at least one cryptography service parameter threshold in said memory includes comparing a size of the cryptographic key with the at least one cryptography service parameter threshold in said memory, wherein the size of the cryptographic key is identified by bit length.) ~~The method as recited in Claim 1, wherein:~~

~~in an event that the cryptography service is an asymmetric cryptography service, the minimum level of security comprises a minimum acceptable public key size of at least 1024 bits; and~~

~~in an event that the cryptography service is a symmetric cryptography service, the minimum level of security comprises a minimum acceptable symmetric key size of at least 128 bits.~~

Allowable Subject Matter

The following is an examiner's statement of reasons for allowance: Applicant's arguments on pg. 24 of the Remarks are persuasive. In particular, the prior art of record does not teach a method or apparatus to establish a minimum and maximum threshold requirement for at least one cryptography service, to determine the relative strength or weakness of a cryptography service requested by a user, and to provide a cryptographic service having a higher level of security than represented by the cryptography service parameter threshold if the requested service does not satisfy the at least one cryptography service parameter threshold in memory. Instead, the prior art discloses defining at least one maximum strength threshold for at least one

cryptographic service; performing a conformance test on the available cryptographic services during initialization of the cryptosystem, determining the relative strength of a cryptographic services requested by a user, and providing an alternative cryptographic service if the cryptographic strength of the requested service exceeds the maximum strength threshold. See Elgamal and Liu. For this reason, claims 1-3, 8-10, 13-16, 18, 19, 22-29, 31, 32, and 34-43 are allowed.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Communications Inquiry

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W. Kim whose telephone number is 571-272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Jung Kim/
Primary Examiner, AU 2432